(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 478 204 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
27.12.2006 Bulletin 2006/52

(51) Int Cl.:
H04Q 7/38 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04L 9/32 *(2006.01)*

(21) Application number: **04252624.4**

(22) Date of filing: **05.05.2004**

(54) **Method and apparatus for performing authentication in a communications system**

Verfahren und Vorrichtung zur Authentifizierung in einem Kommunikationssystem

Procédé et appareil d'authentification dans un système de communications

(84) Designated Contracting States:
DE FR GB

(30) Priority: **15.05.2003 US 438686**

(43) Date of publication of application:
17.11.2004 Bulletin 2004/47

(60) Divisional application:
06023313.7

(73) Proprietor: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventor: **Patel, Sarvar M.**
Montville, NJ 07045 (US)

(74) Representative: **Sarup, David Alexander et al**
Lucent Technologies EUR-IP UK Ltd
Unit 18, Core 3
Workzone
Innova Business Park
Electric Avenue
Enfield, EN3 7XB (GB)

(56) References cited:
WO-A-00/02406 **WO-A-02/052784**
WO-A-20/04032557

- **H. HAVERINEN: "EAP SIM Authentication" IETF, [Online] February 2003 (2003-02), pages 1-52, XP002293906 Retrieved from the Internet: URL: http://www.watersprings.org/pub/id/dra ft-haverinen-pppext-eap-sim-10.txt> [retrieved on 2004-08-24]**

EP 1 478 204 B1

Description

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

[0001] This invention relates generally to a communications system, and, more particularly, to performing authentication in a wireless communications system.

2. DESCRIPTION OF THE RELATED ART

[0002] Masquerading and eavesdropping are potential threats to the security of wireless communications. To provide proper protection for communication over a wireless link, it is desirable to first authenticate the communicating devices and then to encrypt contents of the communications. Several well known protocols have been proposed by standards bodies in recent years to authenticate the identity of the remote party. One such protocol currently under consideration is the Extensible Authentication Protocol for authentication and session key distribution using the Global System for Mobile (GSM) Subscriber Identity Module (SIM). This protocol is hereinafter referred to as the EAP-SIM protocol.

[0003] The EAP-SIM protocol is based on proposed enhancements to existing Global System for Mobile communications authentication procedures. The EAP-SIM protocol specifies a mechanism for mutual authentication and session key agreement using the GSM System Identity Module. For mutual authentication, the client and the server must prove their respective identities to each other before performing any application functions. The central principal of mutual authentication is that neither party must "trust" the other before identity has been proven.

[0004] The GSM network authenticates the identity of the subscriber based on a challenge-response mechanism. The GSM network sends a 128-bit random number (RAND) challenge to a mobile station. The mobile station computes a 32-bit signed response (SRES) and a 64-bit cipher key, K_c, based on the random number (RAND) using an individual subscriber authentication key (K_i). The mobile station then transmits the SRES to the GSM network. Upon receiving the SRES from the mobile station, the GSM network repeats the calculation to verify the identity of the mobile station. Note that the individual subscriber authentication key (K_i) is never transmitted over the radio channel. It is present in the mobile station, as well as in the database of the service network. If the received SRES agrees with the calculated value, the mobile station has been successfully authenticated, and thus, the communication may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the mobile station.

[0005] A specification, entitled "EAP SIM Authentication" (published by IETF, February 2003), provides a method for authentication comprising receiving a request for authentication from a server, the request for authentication including a first and a second random challenge.

[0006] A PCT Application No. WO 00/02406 provides authentication to be performed in an IP network. This reference describes an IP terminal that uses a subscriber identity module (SIM) to generate a response based on a single challenge received.

[0007] The GSM network, as described above, thus utilizes a single RAND challenge to authenticate the identity of the mobile station. The EAP-SIM protocol, based on the authentication procedures of GSM, specifies a mechanism for mutual authentication using a 64-bit cipher key, K_c. Performing mutual authentication based on a 64-bit key, however, may not provide the desired security level as would otherwise be provided by, for example, a 96-bit or a 128-bit key. In an effort to offer a more secure authentication mechanism, the EAP-SIM protocol states that up to three (3) RAND challenges, and thus up to three 64-bit keys K_c, may be utilized during the authentication procedure. The three 64-bit keys, when combined, result in a 192-bit key, which should presumably provide increased security. However, simply combining a plurality of cipher keys does not necessarily result in increased security because an impersonator (or unscrupulous party) may still be able to successfully perform authentication with a mobile station based on correctly guessing the value of a 64-bit key. This is because the EAP-SIM protocol does not require that each RAND challenge (and thus each K_c key) be unique for a given set of triplets. An impersonator can thus establish an unauthorized session, and thereby carry on a full conversation, with a mobile station by first correctly guessing a value of a single 64-bit cipher key and then using multiple copies of that key to authenticate itself to the mobile station.

[0008] The present invention is directed to overcoming, or at least reducing, the effects of, one or more of the problems set forth above.

SUMMARY OF THE INVENTION

[0009] The present invention is characterized over the disclosure of the "EAP SIM Authentication" specification in that comparing the first random challenge and the second random challenge; denying the request for authentication in response to determining that the first random challenge is the same as the second random challenge; and transmitting

an encoded value to the server in response to determining that the first random challenge is different from the second random challenge, wherein the encoded value is generated based on the first and second random challenge and a key that is not shared with the server.

[0010] In one embodiment of the present invention, a method for performing authentication in a communications system is provided. The method includes receiving, at an access terminal, a request for authentication from a server, the request for authentication including a first and a second random challenge, and comparing the first random challenge and the second random challenge. The method further includes denying the request for authentication in response to determining that the first random challenge is the same as the second random challenge, and transmitting an encoded value to the server in response to determining that the first random challenge is different from the second random challenge, wherein the encoded value is generated based on the first and second random challenge and a key that is not shared with the server.

[0011] In one embodiment of the present invention, an apparatus for performing authentication in a communications system is provided. The apparatus includes a receiver adapted to receive a request for authentication from the server, the request for authentication including a first and a second random challenge. The apparatus includes a control unit communicatively coupled to the receiver. The control unit is adapted to compare the first random challenge and the second random challenge, and deny the request for authentication in response to determining that the first random challenge is the same as the second random challenge. The control unit is further adapted to transmit an encoded value to the server in response to determining that the first random challenge is different from the second random challenge, wherein the encoded value is generated based on the first and second random challenge and a key that is not shared with the server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The invention may be understood by reference to the following description taken in conjunction with the accompanying drawings, in which like reference numerals identify like elements, and in which:

Figure 1 is a block diagram illustration of a communications system, in accordance with one embodiment of the present invention;

Figure 2 depicts a block diagram of an access terminal, in accordance with one embodiment of the present invention;

Figure 3 depicts an exemplary message flow diagram of an authentication procedure that is implemented in the communications system of Figure 1, in accordance with one embodiment of the present invention; and

Figure 4 illustrates a flow diagram of a method that may be employed in the communications system of Figure 1, in accordance with one embodiment of the present invention.

[0013] While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and are herein described in detail. It should be understood, however, that the description herein of specific embodiments is not intended to limit the invention to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

[0014] Illustrative embodiments of the invention are described below. In the interest of clarity, not all features of an actual implementation are described in this specification. It will of course be appreciated that in the development of any such actual embodiment, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which will vary from one implementation to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking for those of ordinary skill in the art having the benefit of this disclosure.

[0015] Turning now to the drawings, and specifically referring to Figure 1, a communications system 100 is illustrated, in accordance with one embodiment of the present invention. For illustrative purposes, authentication in the communications system 100 of Figure 1 is performed according to the EAP-SIM protocol, although it should be understood that other authentication protocols may be employed in alternative embodiments. An Internet draft of the EAP-SIM Protocol (February 2003) has been made available by the Internet Engineering Task Force, and is available at http://www.watersprings.org/pub/id/draft-haverinen-pppext-eap-sim-10.txt.

[0016] The communications system 100 of Figure 1 includes a mobile services switching center 110 that allows one

or more access terminals 120 to communicate with a data network 129, such as the Internet, through one or more base stations (BTS) 130. The mobile services switching center 110 of Figure 1 generally provides replication, communications, runtime, and system management services. The mobile services switching center 110 may also handle call processing functions, such as setting and terminating a call path. The access terminal 120 may include one of a variety of devices, including cellular phones, personal digital assistants (PDAs), laptops, digital pagers, wireless cards, and any other device capable of accessing the data network 129.

[0017] An exemplary block diagram of the access terminal 120 is shown in Figure 2, in accordance with one embodiment of the present invention. Although not so limited, in the illustrated embodiment, the access terminal 120 is a GSM cellular telephone handset. The access terminal 120 includes a subscriber identity module (SIM) 121, which includes a control unit 122 and a storage unit 123. In the depicted embodiment, the SIM 121 includes an authentication module 125 for performing authentication procedures in a manner described in greater detail below. The authentication module 125, if implemented in software, may be executable by the control unit 122 and storable in the storage unit 123. Although not shown in Figure 2, the SIM 121 may include an international mobile subscriber identity (IMSI), an individual subscriber authentication key (K_i), a ciphering key generating algorithm (A8), and a personal identification number (PIN). The access terminal 120 in the illustrated embodiment includes transmission/reception logic 126 and an antenna 127 for transmitting and receiving data over a wireless link.

[0018] Referring again to Figure 1, the communications system 100 includes a mobile services switching center 110 that is coupled to an authentication, authorization, and Accounting (AAA) server 140. In the illustrated embodiment, the AAA server 140 includes an EAP server 145, although in alternative embodiments the EAP server 145 may be implemented in a standalone device. The EAP server 145 interfaces with a GSM network 150 and operates as a gateway between the data network 129 and a GSM network 150. The GSM network 150 includes a home location register (HLR) 155 that provides the mobile services switching center 110 with one or more triplets, where each triplet comprises a random (RAND) challenge (*e.g.*, a random number), a signed response (SRES), and a cipher key (K_c). In one embodiment, the RAND is an 128 bit number, and it is used with the individual subscriber authentication key K_i (which may be up to 128 bits long) to generate the cipher key K_c and the SRES value, which are 64 bits and 32 bits long, respectively.

[0019] As described in greater detail below, in accordance with one or more embodiments of the present invention, an improved scheme is provided for performing mutual authentication between the access terminal 120 and the EAP server 145. In accordance with one embodiment of the present invention, the mutual authentication procedure implemented in the communications system 100 offers greater security than that available under some of the existing protocols.

[0020] The data network 129 shown in Figure 1 may be a packet-switched data network, such as a data network according to the Internet Protocol (IP). One version of IP is described in Request for Comments (RFC) 791, entitled "Internet Protocol," dated September 1981. Other versions of IP, such as IPv6, or other connectionless, packet-switched standards may also be utilized in further embodiments. A version of IPv6 is described in RFC 2460, entitled "Internet Protocol, Version 6 (IPv6) Specification," dated December 1998. The data network 129 may also include other types of packet-based data networks in further embodiments. Examples of such other packet-based data networks include Asynchronous Transfer Mode (ATM), Frame Relay networks, and the like.

[0021] As utilized herein, a "data network" may refer to one or more communication networks, channels, links, or paths, and systems or devices (such as routers) used to route data over such networks, channels, links, or paths.

[0022] It should be understood that the configuration of the communications system 100 of Figure 1 is exemplary in nature, and that fewer or additional components may be employed in other embodiments of the communications system 100. For example, the GSM network 150 may also include a visitor location register (not shown) for storing sets of triplets that are generated by the authentication center (AuC) 152. As another example, in one embodiment, the system 100 may include a network management system (not shown) that provides operation, administration, maintenance, and provisioning functions. Additionally, although the mobile services switching center 110 and the AAA server 140 are shown as separate elements, in an alternative embodiment, the functionality of these elements may be performed by a single element.

[0023] Unless specifically stated otherwise, or as is apparent from the discussion, terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical, electronic quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system's memories or registers or other such information storage, transmission or display devices.

[0024] Referring now to Figure 3, one embodiment of an authentication procedure that may be employed in the communications system 100 of Figure 1 is illustrated. The authentication procedure commences with the EAP server 145 providing an identity request (at 205) to the access terminal 120. The access terminal 120 responds (at 210) with an identifier that uniquely identifies the access terminal 120. For example, the access terminal 120 may provide an identifier that includes the International Mobile Subscriber Identity (IMSI) or a temporary identity (pseudonym).

[0025] Following the response provided (at 210) by the access terminal 120, the access terminal receives a start request (at 215) from the EAP server 145. The access terminal 120 responds (at 220) to the received start request.

Through the start request and the start response, the access terminal 120 and the EAP server 145 negotiate a version of a protocol that is supported by both sides. In particular, the start request provided (at 215) by the EAP server 145 contains a Version_List attribute that indicates the version list that is supported by the EAP server 145, and the start response provided (at 220) by the access terminal 120 includes a version attribute that contains the version number that is selected by the access terminal 120. In its start response (at 220), the access terminal 120 also transmits an initial challenge, $RAND_c$, to the EAP server 145.

[0026] Upon receiving the start response (at 220) from the access terminal 120, the EAP server 145 obtains one or more GSM triplets from the Authentication Centre (AuC) 152 of the GSM network 150. In some cases, the GSM triplets may be prefetched by the EAP server 145 in anticipation of possible future use. The EAP-SIM protocol supports using up to three triplets for performing authentication. As noted earlier, each triplet comprises a random (RAND) challenge, a signed response (SRES), and a cipher key (K_c), where the SRES and K_c are calculated based on the RAND value and the K_i key. The EAP server 145 does not specify that the RAND challenges of different triplets must be different.

[0027] Next, the EAP server 145 provides (at 225) a challenge request to the access terminal 120. The challenge request contains one or more RAND challenges and a message authentication code, MAC_k, associated with the one or more of the RAND challenges. Algorithms for calculating MAC values are well known to those skilled in art. One exemplary algorithm for calculating MAC values is described in a reference entitled, "HMAC: Keyed-Hashing for Message Authentication", by H. Krawczyk, M. Bellare, R. Canetti, RFC 2104, February 1997.

[0028] In the authentication procedure illustrated in Figure 3, the MAC_k is calculated based at least on the RAND values from the received triplets and the $RAND_c$ (which was transmitted previously (at 220) by the access terminal 120). For example, assuming that the EAP server 145 transmits two RAND challenges (R1 and R2), the MAC_k is calculated based at least on the R1, R2, and $RAND_c$. The EAP-SIM protocol specifies that an authorization key, *k*, is needed before a MAC value may be calculated. To calculate the authorization key, *k*, a master key (MK) first needs to be calculated. The MK can be calculated using equation (1) below:

$$MK = SHA[\ldots, \text{cipher keys } (K_{c1}, K_{c2}, K_{c3}), RAND_c, \ldots], \qquad (1)$$

where SHA represents a secure hash algorithm, and the cipher keys are part of the GSM triplets, and $RAND_c$ is the initial challenge provided by the access terminal 120. One example of a secure hash algorithm is described in Federal Information Processing Standard (FIPS) Publication 180-1, entitled "Secure Hash Standard," published by National Institute of Standards and Technology, dated April 17, 1995.

[0029] It should be appreciated that the MAC value and master key may be calculated based on other types of information (*e.g.*, version number, identity, etc.) as well; however, for illustrative purposes and to avoid unnecessarily obscuring the described embodiments of the present invention, these details are not described herein.

[0030] The master key (MK), once calculated using equation (1) above, is provided to a pseudo-random number function (PRF) to generate the authorization key, *k*, that, as noted, is needed to calculate the MAC value. An exemplary pseudo-random number function that may be employed is described in a reference entitled, "HMAC: Keyed-Hashing for Message Authentication", by H. Krawczyk, M. Bellare, R. Canetti, RFC 2104, February 1997.

[0031] Once the authentication key, *k*, is calculated, the EAP server 145 determines the MAC value based at least on the RAND challenges (*i.e.*, $RAND_c$ and RAND numbers from the received GSM triplets) that are to be transmitted to the access terminal 120. The calculated MAC value, along with the RAND challenges of one or more of the GSM triplets, is then transmitted (at 225) to the access terminal 120.

[0032] The authentication module 125 (see Figure 2) of the access terminal 120 determines (at 227) if a session can be established with the mobile services switching center 110 (see Figure 1) to access the data network 129 based on the received RAND challenges and the MAC value. The session can be established if the access terminal 120 can authenticate the EAP server 145. As is described below, in accordance with the one embodiment of the present invention, the access terminal 120 establishes a session upon determining that the received MAC value is valid and upon determining that no two of the received RAND challenges are identical (or substantially identical).

[0033] The access terminal 120 verifies the validity of the received MAC value by independently calculating its MAC value of the RAND challenges transmitted by the EAP server 145 and then comparing the calculated MAC value to the received MAC value. Because the initial key, K_i, is available to the access terminal 120, the access terminal 120 can calculate the MAC value in the same manner as it is calculated by the EAP server 145. Under the EAP-SIM protocol, the access terminal 120 can authenticate the EAP server 145 based on determining that the received MAC value is valid. However, authenticating based on the validity of the received MAC value may offer limited security because an unscrupulous party may be able to establish a session with the access terminal 120 by correctly guessing the value of a 64-bit K_c key. That is, by guessing the correct value of K_c, an impersonator can calculate the master key (MK) to derive

the authentication key, *k*, which can then be used to determine the MAC value. The impersonator can transmit the MAC value to the access terminal 120 to authenticate itself, and thereafter carry an unauthorized, full conversation with the access terminal 120. Moreover, transmitting multiple RAND challenges of multiple GSM triplets, as allowed by the EAP-SIM protocol, does not necessarily make the authentication procedure more secure because there is no restriction that each of the RAND challenges be unique. Thus, the impersonator can correctly guess a value of a K_c for a given RAND challenge, calculate the master key based on multiple copies of K_c, and then calculate a valid MAC value based on the master key.

[0034] To reduce the possibility of an unauthorized access, two embodiments are described herein. The first embodiment is illustrated in Figure 4, which illustrates a flow diagram of the block 227 of Figure 3, in accordance with one embodiment of the present invention. For illustrative purposes, it is herein assumed that the EAP server 145 transmits multiple RAND challenges, and a MAC value of these RAND challenges for authentication purposes. Referring to Figure 4, the authentication module 125 (see Figure 2) determines (at 405) if any two of the received RAND challenges are the same. If no two RAND challenges are the same (or, put another way, if all of the RAND challenges are unique), then the authentication module 125 determines (at 410) if the MAC value received from the EAP server 145 is valid. As noted, the access terminal 120 can determine (at 410) the validity of the received MAC value by independently calculating its own MAC value of the RAND challenges transmitted by the EAP server 145 and then comparing the calculated MAC value to the received MAC value. If the MAC values do not match, then the access terminal 120 ignores (at 412) the challenge request received (see reference 225 of Figure 3) from the EAP server 145. If a valid MAC value is not received within a prescribed amount of time, no connection is established because of authentication failure.

[0035] If the authentication module 125 determines (at 410) that the received MAC value is valid, the authentication module 125 calculates (at 415) the SRES values based on the received RAND challenges and then determines a MAC value of the SRES values. In an alternative embodiment, the authentication module 125 may determine a MAC value based on other information, such as cipher keys, RAND challenges, and the like. The MAC value is then transmitted (at 417) to the EAP server 145 in a response-to-challenge packet (see reference numeral 230 of Figure 3). The EAP server 145, upon receiving the MAC value from the access terminal 120, verifies the validity of the MAC value, and, if the MAC value is determined to be valid, transmits a success signal (see reference numeral 245 of Figure 3) to the access terminal 120. Upon receiving the success signal, the authentication module 125 allows (at 420) a session to be established between the access terminal 120 and the mobile services switching center (110, see Figure 1).

[0036] If the authentication module 125 determines (at 405) that at least two of the MAC values received from the EAP server 145 are identical, the authentication module 125 requires the EAP server 145 to transmit unique, valid RAND challenges before a session can be established with the access terminal 120. Requiring each of the RAND challenges to be unique makes the authentication procedure more secure as an unscrupulous party must correctly guess at least two different values (*e.g.*, K_c keys) to establish a connection with the access terminal 120.

[0037] If it is determined (at 405) that the MAC values from the EAP server 145 are not unique, then the authentication module 145 may cause the EAP to transmit new RAND challenges in one of several ways. In one embodiment, the authentication module 125 may ignore (at 425) the challenge request (see reference numeral 225 of Figure 3) from the EAP server 145. Upon an expiration of a preselected amount of time, the EAP server 145 may transmit new RAND challenges, along with their MAC value. In an alternative embodiment, the authentication module 125 may reject (at 430) the challenge request from the EAP server 145, thereby requiring the EAP server 145 to transmit new RAND challenges as well as their MAC value. In yet another alternative embodiment, the authentication module 125 allows (at 435) a connection to be established with the access terminal 120 and thereafter terminates the connection, thus requiring the EAP server 145 to transmit new RANDs and an associated MAC value.

[0038] Thus, in accordance with one or more embodiments of the present invention, the authentication procedure is more secure if the access terminal requires each of the received RAND challenges to be different from each other. This approach may be employed within the context of the EAP-SIM protocol without requiring substantial, or any, changes to the proposed EAP-SIM protocol. An alternative embodiment of securing the authenticating procedure of Figure 3 includes requiring the signed response (SRES) to be part of the master key (MK) calculation. Thus, equation (1) above may be re-written as equation (2) below:

$$MK = SHA[\ldots, \text{cipher keys } (K_{c1}, K_{c2}, K_{c3}), SRES_1, SRES_2, SRES_3, RAND_c, \ldots]. \quad (2)$$

[0039] Defining the master key to include the SRES value(s) makes the authentication more secure because it requires an unscrupulous party to not only guess the correct value of K_c but also the SRES value(s). While equation (2) assumes that the EAP server 145 utilizes three GSM triplets (because of the terms K_{c1}, K_{c2}, K_{c3}, $SRES_1$, $SRES_2$, and $SRES_3$), this equation can readily be modified accordingly for use with a single triplet or any other number of triplets. Using equation (2) for calculating the MK makes the authentication procedure more secure even if only one triplet (and thus

one RAND challenge) is employed because it requires the adversary to correctly guess not only the value of the K_C but also the SRES value. This alternative embodiment of modifying the MK calculation may require a change to the EAP-SIM protocol insofar as the EAP-SIM protocol defines the algorithm for calculating the master key.

[0040] In one embodiment, equation (2) may be employed in lieu of equation (1) for the authentication procedure described in Figures 3 and 4. That is, in one embodiment, the authentication procedure may include requiring the master key calculation to include the SRES value(s) (as shown in equation (2)) and it may further include requiring the EAP server 145 to transmit unique RAND challenges in instances multiple GSM triplets are employed.

[0041] While Figure 3 illustrates a mutually authentication procedure, it should be appreciated that one or more of the above-described embodiments of the present invention may also be applicable to a unilateral authentication procedure. In a unilateral authentication procedure, the EAP server 145 may, for example, authenticate the access terminal 120 by transmitting one or more RAND challenges to the access terminal 120, where the access terminal 120 then responds to the received RAND challenges.

[0042] For illustrative purposes, one or more embodiments of the present invention are described in the context of a wireless communications system. However, it should be appreciated that in alternative embodiments the present invention may also be implemented in wired networks. Additionally, the present invention may also be applicable to a system supporting voice-only communications or voice and data communications.

[0043] Those skilled in the art will appreciate that the various system layers, routines, or modules illustrated in the various embodiments herein may be executable control unit (such as the control unit 122 (see Figure 2)). The control unit 122 may include a microprocessor, a microcontroller, a digital signal processor, a processor card (including one or more microprocessors or controllers), or other control or computing devices. The storage devices referred to in this discussion may include one or more machine-readable storage media for storing data and instructions. The storage media may include different forms of memory including semiconductor memory devices such as dynamic or static random access memories (DRAMs or SRAMs), erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs) and flash memories; magnetic disks such as fixed, floppy, removable disks; other magnetic media including tape; and optical media such as compact disks (CDs) or digital video disks (DVDs). Instructions that make up the various software layers, routines, or modules in the various systems may be stored in respective storage devices. The instructions when executed by a respective control unit 220 causes the corresponding system to perform programmed acts.

[0044] The particular embodiments disclosed above are illustrative only, as the invention may be modified and practiced in different but equivalent manners apparent to those skilled in the art having the benefit of the teachings herein. Furthermore, no limitations are intended to the details of construction or design herein shown, other than as described in the claims below. Accordingly, the protection sought herein is as set forth in the claims below.

Claims

1. A method for authentication in a communications system (100), the method comprising:

   receiving, at an access terminal (120), a request for authentication from a server (145), the request for authentication including a first and a second random challenge,

   characterized by,:
   comparing the first random challenge and the second random challenge;
   denying the request for authentication in response to determining that the first random challenge is the same as the second random challenge; and
   transmitting an encoded value to the server (145) in response to determining that the first random challenge is different from the second random challenge, wherein the encoded value is generated based on the first and second random challenge and a key that is not shared with the server (145).

2. The method of claim 1, wherein denying the request for authentication comprises performing at least one of not responding to the request for authentication, rejecting the request from the server (145), and establishing a session for at least one of voice and data communications and terminating the session.

3. The method of claim 1, further comprising receiving a message authentication code associated with at least the first random challenge and the second random challenge in response to transmitting an initial random challenge to the server (145).

4. The method of claim 3, further comprising verifying if the received message authentication code is valid and further

comprising establishing a communications session based on determining that the message authentication code is valid.

5. The method of claim 4, wherein verifying the received message authentication code comprises:

determining a master key based on one or more cipher keys associated with the first random challenge and the second random challenge;
calculating a message authentication code based on the master key; and
comparing the calculated message authentication code and the received message authentication code.

6. The method of claim 5, wherein receiving the request for authentication comprises receiving the request for authentication including a third random challenge and wherein denying the request for authentication comprises denying the request if any two of the received random challenges are the same.

7. An apparatus (120) for performing authentication in a communications system (100), the apparatus comprising:

a receiver (126) adapted to receive a request for authentication from a server (145), the request for authentication including a first and a second random challenge,

characterized by,:
a control unit (122) communicatively coupled to the receiver, the control unit (122) adapted to:

compare the first random challenge and the second random challenge;
deny the request for authentication in response to determining that the first random challenge is the same as the second random challenge; and
transmit an encoded value to the server (145) in response to determining that the first random challenge is different from the second random challenge, wherein the encoded value is generated based on the first and second random challenge and a key that is not shared with the server (145).

8. The apparatus (120) of claim 7, wherein the control unit (122) is adapted to at least one of ignore the request for authentication based on determining that the first random challenge is not equal to the second random challenge, reject the request from the server based on determining that the first random challenge is not equal to the second random challenge, and establish a session for at least one of voice and data communications and to terminate the session based on determining that the first random challenge is not equal to the second random challenge.

9. The apparatus (120) of claim 8, wherein the control unit (122) is adapted to receive a message authentication code associated with the first random challenge and the second random challenge.

Patentansprüche

1. Verfahren zur Authentifizierung in einem Kommunikationssystem (100), umfassend die Schritte:

Empfangen an einem Zugriffsterminal (120) einer Aufforderung zur Authentifizierung von einem Server (145), wobei die Aufforderung zur Authentifizierung eine erste und eine zweite zufällige Ziffernfolge umfasst, **gekennzeichnet durch** Folgendes:

Vergleichen der ersten zufälligen Ziffernfolge mit der zweiten zufälligen Ziffernfolge; Ablehnen der Aufforderung zur Authentifizierung als Antwort auf die Feststellung, dass die erste zufällige Ziffernfolge dieselbe wie die zweite zufällige Ziffernfolge ist; und
Übertragen eines codierten Wertes zum Server (145) als Antwort auf die Feststellung, dass sich die erste zufällige Ziffernfolge von der zweiten zufälligen Ziffernfolge unterscheidet, wobei der codierte Wert generiert wird auf der Basis der ersten und zweiten zufälligen Ziffernfolge und einem Schlüssel, der nicht gemeinsam mit dem Server (145) genutzt wird.

2. Verfahren nach Anspruch 1, wobei das Ablehnen der Aufforderung zur Authentifizierung das Ausführen mindestens eines der folgenden Schritte umfasst: das Geben keiner Antwort auf die Aufforderung zur Authentifizierung, das Zurückweisen der Aufforderung vom Server (145) oder das Eröffnen einer Sitzung für mindestens eine der Sprech-

und Datenkommunikationen und Beenden der Sitzung.

3. Verfahren nach Anspruch 1, ferner umfassend das Empfangen eines Codes zur Authentifizierung einer Nachricht in Zusammenhang mit mindestens der ersten zufälligen Ziffernfolge und der zweiten zufälligen Ziffernfolge als Antwort, auf die Übertragung einer ersten zufälligen Ziffernfolge zum Server (145).

4. Verfahren nach Anspruch 3, ferner umfassend das Überprüfen, ob der empfangene Code zur Authentifizierung einer Nachricht gültig ist und ferner umfassend das Eröffnen einer Kommunikationssitzung, die darauf basiert, festzustellen, dass der Code zur Authentifizierung einer Nachricht gültig ist.

5. Verfahren nach Anspruch 4, wobei das Überprüfen des Codes zur Authentifizierung einer Nachricht Folgendes umfasst:

Ermitteln eines Hauptschlüssels, basierend auf einem oder mehreren Chiffrierschlüsseln in Zusammenhang mit der ersten zufälligen Ziffernfolge und der zweiten zufälligen Ziffernfolge;
Errechnen eines Codes zur Authentifizierung einer Nachricht auf der Basis des Hauptschlüssels; und
Vergleichen des errechneten Codes zur Authentifizierung einer Nachricht und des empfangenen Codes zur Authentifizierung einer Nachricht.

6. Verfahren nach Anspruch 5, wobei das Empfangen der Aufforderung zur Authentifizierung das Empfangen der Aufforderung zur Authentifizierung, beinhaltend eine dritte zufällige Ziffernfolge umfasst und wobei das Ablehnen der Aufforderung zur Authentifizierung das Ablehnen der Aufforderung umfasst, wenn irgendwelche der beiden empfangenen zufälligen Ziffernfolgen gleich sind.

7. Gerät (120) zum Ausüben der Authentifizierung in einem Kommunikationssystem (100), wobei das Gerät umfasst:

einen Empfänger (126), der zum Empfang einer Aufforderung zur Authentifizierung von einem Server (145) angepasst ist, wobei die Aufforderung zur Authentifizierung eine erste und eine zweite zufällige Ziffernfolge umfasst, **gekennzeichnet durch**:

eine Steuereinheit (122), die kommunikationsfähig an den Empfänger gekoppelt ist, wobei die Steuereinheit (122) angepasst ist, um:

die erste zufällige Ziffernfolge und die zweite zufällige Ziffernfolge zu vergleichen;
die Aufforderung zur Authentifizierung als Antwort auf die Feststellung abzulehnen, dass die erste zufällige Ziffernfolge dieselbe wie die zweite zufällige Ziffernfolge ist, und
Übertragen eines codierten Wertes zum Server (145) als Antwort auf die Feststellung, dass sich die erste zufällige Ziffernfolge von der zweiten zufälligen Ziffernfolge unterscheidet, wobei der codierte Wert generiert wird, basierend auf der ersten und zweiten zufälligen Ziffernfolge und einem Schlüssel, der nicht gemeinsam mit dem Server (145) genutzt wird.

8. Gerät (120) nach Anspruch 7, wobei die Steuereinheit (122) angepasst ist, um mindestens einen der folgenden Schritte auszuführen: die Aufforderung zur Authentifizierung zu ignorieren, basierend auf der Feststellung, dass die erste zufällige Ziffernfolge nicht gleich der zweiten zufälligen Ziffernfolge ist, die Aufforderung vom Server zurückzuweisen, basierend auf der Feststellung, dass die erste zufällige Ziffernfolge nicht gleich der zweiten zufälligen Ziffernfolge ist und eine Sitzung für mindestens eine der Sprech- und Datenkommunikationen zu eröffnen und die Sitzung zu beenden, basierend auf der Feststellung, dass die erste zufällige Ziffernfolge nicht gleich der zweiten zufälligen Ziffernfolge ist.

9. Gerät (120) nach Anspruch 8, wobei die Steuereinheit (122) angepasst ist, um einen Code zur Authentifizierung einer Nachricht in Zusammenhang mit der ersten zufälligen Ziffernfolge und der zweiten zufälligen Ziffernfolge zu empfangen.

Revendications

1. Procédé d'authentification dans un système de communications (100), le procédé comprenant :

la réception, au niveau d'un terminal d'accès (120), d'une requête d'authentification par un serveur (145), la requête d'authentification comportant une première et une deuxième interrogation aléatoire,

caractérisé par :

la comparaison de la première interrogation aléatoire et de la deuxième interrogation aléatoire ;
le refus de la requête d'authentification en réponse à la détermination que la première interrogation aléatoire est identique à la deuxième interrogation aléatoire ; et
la transmission d'une valeur codée au serveur (145) en réponse à la détermination que la première interrogation aléatoire est différente de la deuxième interrogation aléatoire, où la valeur codée est générée d'après les première et deuxième interrogations aléatoires, et une clé qui n'est pas partagée avec le serveur (145).

2. Procédé selon la revendication 1, dans lequel le refus de la requête d'authentification comprend l'exécution d'au moins l'une des opérations de non-réponse à la requête d'authentification, de rejet de la requête du serveur (145), et d'établissement d'une session pour au moins l'une de communications de voix et de données et arrêt de la session.

3. Procédé selon la revendication 1, comprenant en outre la réception d'un code d'authentification de message associé au moins à la première interrogation aléatoire et à la deuxième interrogation aléatoire en réponse à la transmission d'une interrogation aléatoire initiale au serveur (145).

4. Procédé selon la revendication 3, comprenant en outre la vérification si le code d'authentification de message reçu est valable et comprenant en outre l'établissement d'une session de communications d'après la détermination de la validité du code d'authentification de message.

5. Procédé selon la revendication 4, dans lequel le code d'authentification du message reçu comprend :

la détermination d'une clé principale d'après une ou plusieurs clés de chiffrage associées à la première interrogation aléatoire et à la deuxième interrogation aléatoire ;
le calcul d'un code d'authentification de message d'après la clé principale ; et
la comparaison du code d'authentification de message calculé et du code d'authentification de message reçu.

6. Procédé selon la revendication 5, dans lequel la réception de la requête d'authentification comprend la réception de la requête d'authentification comportant une troisième interrogation aléatoire et dans lequel le refus de la requête d'authentification comprend le refus de la requête si deux quelconque des interrogations aléatoires reçues sont identiques.

7. Appareil (120) pour exécuter une authentification dans un système de communications (100), l'appareil comprenant :

un récepteur (126) adapté pour recevoir une requête d'authentification par un serveur (145), la requête d'authentification comportant une première et une deuxième interrogation aléatoire, **caractérisé par** :

une unité de commande (122) couplée pour communiquer avec le récepteur, l'unité de commande (122) étant adaptée pour :

comparer la première interrogation aléatoire et la deuxième interrogation aléatoire ;
refuser la requête d'authentification en réponse à la détermination que la première interrogation aléatoire est identique à la deuxième interrogation aléatoire ; et
transmettre une valeur codée au serveur (145) en réponse à la détermination que la première interrogation aléatoire est différente de la deuxième interrogation aléatoire, où la valeur codée est générée d'après les première et deuxième interrogations aléatoires, et une clé qui n'est pas partagée avec le serveur (145).

8. Appareil (120) selon la revendication 7, dans lequel l'unité de commande (122) est adaptée pour au moins l'une des opérations consistant à ignorer la requête d'authentification lorsqu'il est déterminé que la première interrogation aléatoire n'est pas identique à la deuxième interrogation aléatoire, rejeter la requête du serveur lorsqu'il est déterminé que la première interrogation aléatoire n'est pas identique à la deuxième interrogation aléatoire, et établir une session pour au moins l'une de communications de voix et de données, et arrêter la session lorsqu'il est déterminé que la première interrogation aléatoire n'est pas identique à la deuxième interrogation aléatoire.

9. Appareil (120) selon la revendication 8, dans lequel l'unité de commande (122) est adaptée pour recevoir un code d'authentification de message associé à la première interrogation aléatoire et à la deuxième interrogation aléatoire.

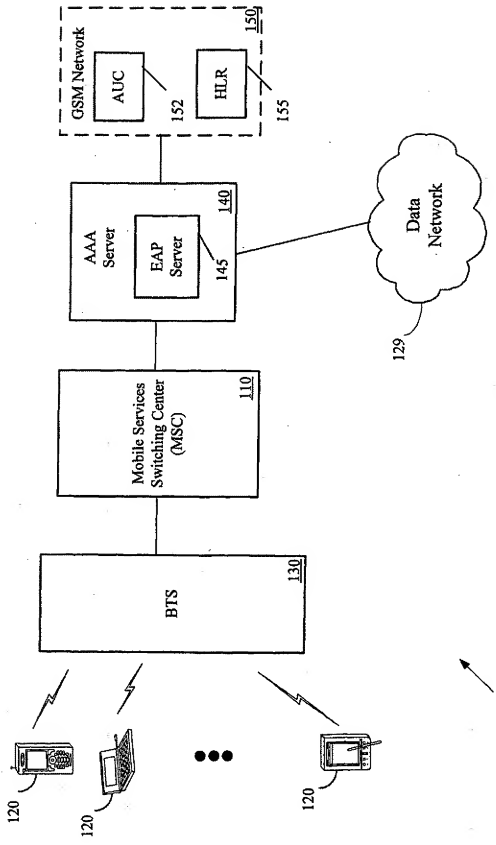
GSM Network
AUC
HLR
150
152
155
AAA Server
EAP Server
140
145
Data Network
129
Mobile Services Switching Center (MSC)
110
BTS
130
120
120
120
100

FIGURE 1

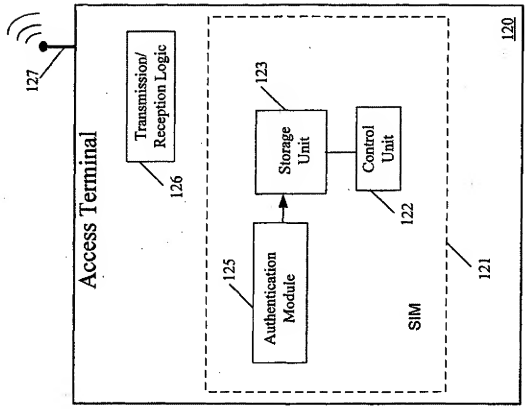
127
Access Terminal
Transmission/
Reception Logic
126
123
Storage
Unit
Control
Unit
122
125
Authentication
Module
SIM
121
120

FIGURE 2

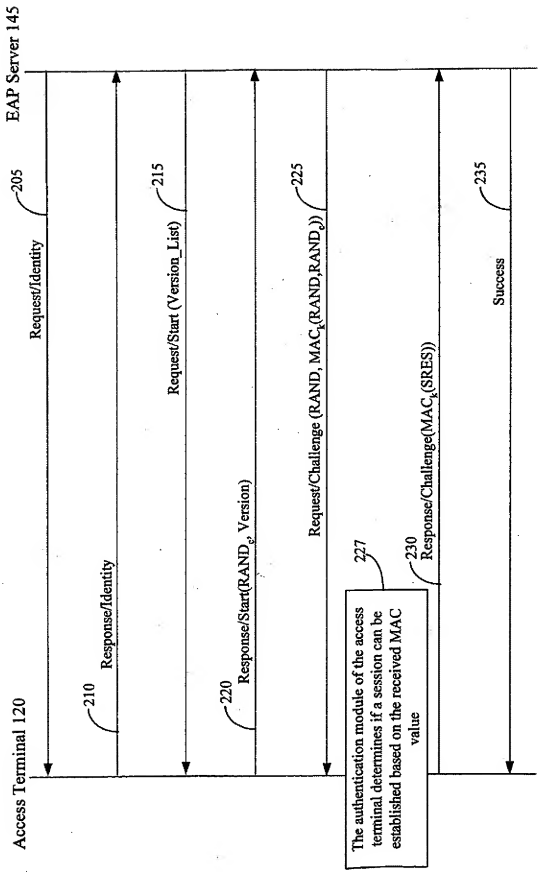
Access Terminal 120
EAP Server 145
Request/Identity
205
210
Response/Identity
Request/Start (Version_List)
215
220
Response/Start(RAND_e, Version)
Request/Challenge (RAND, MAC_k(RAND,RAND_e))
225
The authentication module of the access terminal determines if a session can be established based on the received MAC value
227
230
Response/Challenge(MAC_k(SRES))
Success
235

FIGURE 3

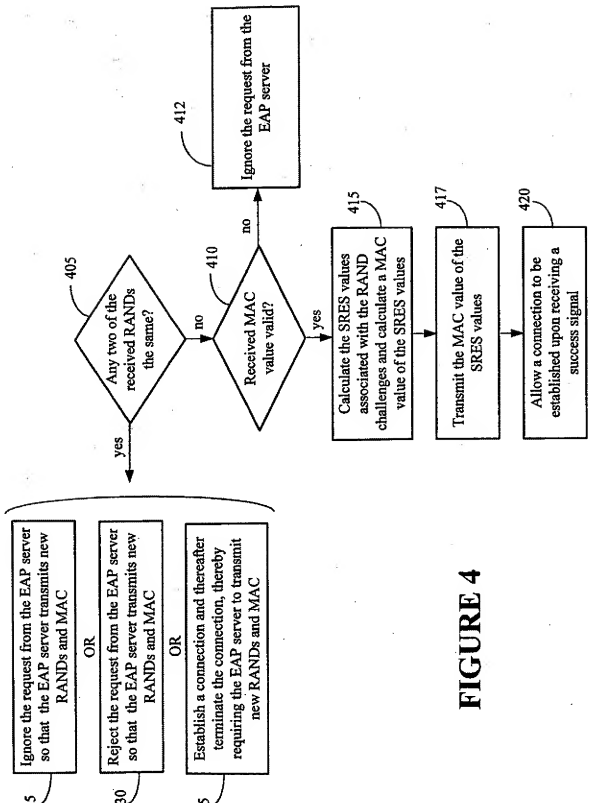
Any two of the received RANDs the same?
405
yes
no
Received MAC value valid?
410
no
yes
412
Ignore the request from the EAP server
Calculate the SRES values associated with the RAND challenges and calculate a MAC value of the SRES values
415
Transmit the MAC value of the SRES values
417
Allow a connection to be established upon receiving a success signal
420
Ignore the request from the EAP server so that the EAP server transmits new RANDs and MAC
OR
Reject the request from the EAP server so that the EAP server transmits new RANDs and MAC
OR
Establish a connection and thereafter terminate the connection, thereby requiring the EAP server to transmit new RANDs and MAC
425
430
435

FIGURE 4